Annual 47 C.F.R. & 64.2009(e) CPNI Certification for 2012
EB Docket 06-36

Date filed:	February 29, 2012
Name of company covered by this certification:	Momentum Telecom, Inc. 2700 Corporate Drive Suite 200 Birmingham, AL 35242
Form 499 Filer ID:	821474
Name of signatory:	Charles E. Richardson III
Title of signatory:	Vice President and Secretary

I, Charles E. Richardson III, certify that I am an officer Momentum Telecom, Inc. ("Company"), and that acting as an agent of the company, I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with CPNI rules promulgated by the Federal Communications Commission ("Commission") and set forth in 47 CFR, Chapter I, Part 64, Subpart U (the "CPNI Rules").

Actions Against Data Brokers

The Company **has not** instituted proceedings, filed petitions, or initiated comparable action before a state commission, a court system, or the Commission against data brokers in the past year.

Customer Complaints

The Company **has not** received customer complaints in the past year concerning the unauthorized release of CPNI.

Explanation of Operating Procedures

In accordance with the requirements set forth in 47 CFR §64.2009(e), attached to this certificate is a statement explaining how the Company's operating procedures ensure that the Company is in compliance with the requirements set forth in the CPNI Rules.

Charles E. Richardson III
Vice President and Secretary

Attachment

Annual 47 C.F.R. 64.2009(e) CPNI Certification
EB Docket 06-36

Statement Concerning CPNI Operating Procedures
(submitted Pursuant to 47 CFR §64.2009(e))

Momentum Telecom, Inc.
2700 Corporate Drive Suite 200
Birmingham, AL 35242

To ensure compliance with the provisions of 47 CFR, Chapter I, Part 64, Subpart U (the "CPNI Rules"), the Company has adopted practices that are consistent with the highly sensitive nature of CPNI, the text and purpose of the CPNI Rules, and the limited use of CPNI by the Company. These practices include:

- Educating Company personnel regarding authorized and unauthorized use of CPNI, circumstances under which CPNI may be shared and procedures that must be followed, and protecting CPNI from inadvertent or accidental disclosure to unauthorized third parties.

  This instruction is intended to ensure that Company personnel: (a) know what constitutes CPNI; (b) understand and participate in the Company's efforts to protect CPNI; (c) know when they are, and are not, authorized to use CPNI; (d) confirm that each customer has consented to the use of CPNI for marketing purposes in accordance with Company procedures before using CPNI for such purposes; and (e) are aware of and comply with record keeping requirements applicable to customer complaints concerning CPNI, and the use of CPNI for marketing purposes.

- Taking appropriate disciplinary action in cases where Company personnel fail to follow such practices.

- Using authentication techniques that do not incorporate CPNI or other readily available biographical information to identify customers before permitting online access to, or communicating verbally with regard to a customer account. The Company may negotiate alternative authentication procedures for business customers that have both a dedicated account representative and a contract that specifically addresses the protection of CPNI.

- Except as otherwise required by law, prohibiting the disclosure of CPNI (a) to third parties other than Company Affiliates, and (b) to an Affiliate of the Company, unless the relevant customer has subscribed to a service that is provided by such Affiliate.

- The Company will electronically report CPNI breaches within 7 days to the US Secret Service and the FBI through the designated central reporting facility at https://www.cpnireporting.gov. Following electronic notification to the designated central reporting facility, an affected customer will be promptly notified by mail unless the Company is otherwise instructed by law enforcement.

- Prohibiting the use of CPNI for the purpose of marketing new categories of service to existing customers without first obtaining such customer's consent to the use of CPNI for such purposes.

- Maintaining records of the sales and marketing campaigns executed by the Company and its Affiliates that use CPNI.

- Restricting decisions regarding the use and disclosure of CPNI to Company management, and requiring Company management oversee opt-in, opt-out, and other customer approval and customer notice processes.

- Promptly notifying customers by mail whenever a password, customer response to a backup means of authentication for lost or stolen passwords, online account, or address of record is created or changed. This notification is not provided when the customer initiates service, including the selection of a password at service initiation.

- Employing reasonable measures to discover and protect against unauthorized access to CPNI.